

## THE NATURAL NUMBERS

We are ready for the official introduction of the natural numbers. I ask you to suspend belief in the truth of the things you already know about the natural numbers. I insist you keep every bit of your knowledge - just stop taking things for granted. “The Natural Numbers” is now a name only, to be used in the following list of mathematical statements, each of which you are asked to regard as true.

This is where the course *really* starts. What came before was “preliminary.” We still have some preliminary stuff to do. But the natural numbers will literally be the foundation on which are built the ordinary integers, the rational numbers, and then the real and the complex numbers, which all form the foundations for Calculus.

### (01) The Peano Postulates (or Axioms)

We assume that the four following mathematical statements are true.

- (01A) There exists a non-empty set  $\mathbb{N}$ , whose elements we will call *natural numbers*.
- (01B) There exists a one-to-one function  $s : \mathbb{N} \rightarrow \mathbb{N}$ , that we will call the *successor function*.
- (01C) There exists an element  $0 \in \mathbb{N}$  such that  $0$  is not in the image,  $s(\mathbb{N})$ , of  $s$ .
- (01D) For all subsets  $S$  of  $\mathbb{N}$ , if  $S$  contains  $0$ , and  $s(S) \subseteq S$ , then  $S = \mathbb{N}$ .

Here is a restatement of these axioms, in a less dense form:

- (02-1) There exists a non-empty set  $\mathbb{N}$ , called the set of natural numbers, and a function  $s$  on  $\mathbb{N}$ , called the successor function, whose value,  $s(n)$ , at any  $n$  in  $\mathbb{N}$ , is called the successor of  $n$ , such that
- (02-2) Different elements of  $\mathbb{N}$  have different successors ( $s$  is one-to-one),
- (02-3) There is an element,  $0$ , of  $\mathbb{N}$  that is not the successor of any element of  $\mathbb{N}$  ( $0$  is not in the image of  $s$ ),
- (02-4) Every subset  $S$  of  $\mathbb{N}$  that contains  $0$  and also contains the successor of each element of  $S$  must be equal to  $\mathbb{N}$  (if  $S$  contains  $0$ , and  $s(S) \subseteq S$ , then  $S = \mathbb{N}$ ).

According to the Encyclopedia Britannica, 15th edition, the five Peano postulates are:

1.  $0$  is a number.
2. The successor of any number is also a number.
3. No two distinct numbers have the same successor.
4.  $0$  is not the successor of any number.
5. If any property is possessed by  $0$  and also by the successor of any number having that property, then all numbers have that property.

Postulate 5, (01D) and (02-4) are certainly different. But all three versions amount to the same thing mathematically, when expressed in terms of set-selector notation. For, “property” has to refer to a mathematical statement  $P(n)$  about elements  $n$  of  $\mathbb{N}$ . Thus,  $\{n \in \mathbb{N} : P(n) \text{ is true}\}$  is the set of all elements of  $\mathbb{N}$  that possess the property  $P(n)$ . If the “property” satisfies the conditions of postulate 5, then  $0 \in \{n \in \mathbb{N} : P(n) \text{ is true}\}$ , and

$$s(\{n \in \mathbb{N} : P(n) \text{ is true}\}) \subseteq \{n \in \mathbb{N} : P(n) \text{ is true}\},$$

so  $\{n \in \mathbb{N} : P(n) \text{ is true}\} = \mathbb{N}$ . On the other hand, let  $S$  be a subset of  $\mathbb{N}$ . We define the “property (of  $n$ )” to be that  $n$  belongs to  $S$ . That is,  $P(n)$  is the statement “ $n \in S$ .” This “property” is then covered by postulate 5.

Postulate 5 is about *sets* of natural numbers. You probably did not bring this postulate with you to this course, at least not explicitly. And yet, it will seem natural to you shortly, I hope. Here are the three versions of Postulate 5, collected in one place:

For all subsets  $P$  of  $\mathbb{N}$ , if  $P$  contains the element  $0$ , and  $s(P) \subseteq P$ , then  $P = \mathbb{N}$ ;

Every subset of  $\mathbb{N}$  that contains  $0$  and also contains the successor of each of its elements must be equal to  $\mathbb{N}$ ;

If any property is possessed by  $0$  and also by the successor of any number having that property, then all numbers have that property.

This Postulate is called **The Principle of Mathematical Induction**.

The Principle of Mathematical Induction is our principal source of “mathematical energy!”

We usually don’t make axioms in a vacuum - there is usually some thought behind them. But that thought can be hidden! So here is an “explanation” of the axioms. First, let’s imagine that we go into the “back room,” where we don’t have to prove anything - just work on ideas! We “know” the integers exist, positive, zero and negative. The natural numbers are going to be our model of the non-negative integers. The successor function is “really” the function whose value at  $n$ ,  $n \geq 0$ , is  $n + 1$ :  $s(n) = n + 1$ . Different non-negative integers “should” have different successors. This is what “ $s$  is one-one” means. This is an assumption about the successor function! Saying 0 is not the successor of any non-negative integer means that  $0 \neq n + 1$  for any non-negative integer  $n$ . The postulate about sets of non-negative integers is not something we usually take for granted. But the idea makes sense: if a set  $S$  contains 0, and contains the successor of each of its elements, then it also contains 1, and 2, and 3, and so on. So it ought to contain every non-negative integer, namely  $S = \mathbb{N}$ .

In your experience, perhaps  $\mathbb{N}$  starts with 1, not 0. There is an equivalent version of these axioms for that version of  $\mathbb{N}$ . We simply replace each “0” in the first version with “1,” and call the new set  $\mathbb{P}$ , for positive integers. We will want to use induction “starting with 1.” But, instead of making another set of axioms, we can give the name 1 to  $s(0)$ , and then we can deduce the proposed axioms, from the Peano Postulates, so they become a Theorem: a set of true mathematical statements whose truth is logically deduced from axioms, instead of being assumed.

**(03) Theorem and Definition and Notation:** *There is a non-empty set  $\mathbb{P}$ , whose elements we will call positive integers, a one-to-one function  $s : \mathbb{P} \rightarrow \mathbb{P}$ , that we will call the successor function, and an element  $1 \in \mathbb{P}$  such that 1 is not in the image,  $s(\mathbb{P})$ , of  $s$ . In addition, for all subsets  $E$  of  $\mathbb{P}$ , if  $E$  contains 1, and  $s(E) \subseteq E$ , then  $E = \mathbb{P}$ .*

The idea of the proof is to remove 0 from  $\mathbb{N}$  to construct  $\mathbb{P}$ :  $\mathbb{P} := \mathbb{N} \setminus \{0\}$ . Then we have to check that each of the postulates can be re-interpreted in the new set. The Induction property is deduced by temporarily putting 0 back, then taking it out after applying the Principle of Mathematical Induction for  $\mathbb{N}$ . We will not carry out the details of this proof unless you ask.

You have probably seen Mathematical Induction before, but it looked a little different then.

**Example (unofficial!):** Use Mathematical Induction (school version) to show that for all positive integers  $n$ ,  $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ . In this Example, we will use your prior knowledge about  $\mathbb{P}$ .

The procedure is this:

1. Let  $P(n)$  denote the statement to be proved:  $P(n)$  must have  $n$  as its only free variable.
2. Verify that  $P(1)$  is true.
3. Show that, by assuming  $P(n)$  is true, you can deduce that  $P(n + 1)$  must be true.

That is, prove the quantified mathematical statement “For all  $n$  in  $\mathbb{N}$ ,  $P(n) \Rightarrow P(n + 1)$ .”

Then Mathematical Induction assures us that  $P(n)$  is true for all  $n$ .

Let’s do it, for review.

Step 1. Let  $P(n)$  denote the statement “ $1 + 2 + 3 + \cdots + n = n(n + 1)/2$ .” Step 2.  $P(1)$  is the statement “ $1 = 1(1 + 1)/2$ .” This is true, by a very quick computation.

Step 3. Assume that  $P(n)$  is true for some  $n$ . Then  $P(n + 1)$  is the statement “ $1 + 2 + 3 + \cdots + (n + 1) = (n + 1)(n + 2)/2$ .” We have  $1 + 2 + 3 + \cdots + (n + 1) = 1 + 2 + 3 + \cdots + n + (n + 1) = (1 + 2 + 3 + \cdots + n) + (n + 1) = \frac{n(n+1)}{2} + 2\frac{n+1}{2} = \frac{(n+1)(n+2)}{2}$ , by a few basic algebraic manipulations. The equality of the first and last expressions in this chain of equalities is  $P(n + 1)$ , shown to be true under the assumption that  $P(n)$  is true. The truth of  $P(n)$  for all  $n$  is now established, by Mathematical Induction.

**Remark:** Note that, were  $P(n)$  false, the statement  $P(n) \Rightarrow P(n + 1)$  would be true vacuously. Thus we can eliminate that possibility, and concentrate on what happens if  $P(n)$  is true.

The way we will often “do” Mathematical Induction differs only a little from this (and you may certainly use the old way in your papers in this class). The set-theoretic version of the argument for this example:

Let  $E := \{n \in \mathbb{P} : 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}\}$ . We show  $1 \in E$  (just as we just did), and that  $n \in E$  implies  $n + 1 \in E$  (just as we just did). Then  $E = \mathbb{P}$  by Mathematical Induction.

**A digression** You will need to learn new ways to use (the Principle of) Mathematical Induction. You are probably familiar with Mathematical Induction as a tool for verifying formulas. We will need to use Mathematical Induction for other purposes. For example, we will need to know whether certain kinds of functions from  $\mathbb{N}$  to  $\mathbb{N}$  exist. There may be one function for each  $n$ , or maybe our statement will be that there is NO such function, for ANY  $n$ . We will then construct a set

$$S := \{n \in \mathbb{N} : \text{a function } f_n : \mathbb{N} \rightarrow \mathbb{N} \text{ exists such that "thus and so" is true about } f_n\}.$$

Then we will follow the “same” pattern as in school induction:

Step 0: Show that 0 is in  $S$ . *The way we show that 0 is in  $S$  will depend on what the criterion is for membership in  $S$ .* But the *objective* of Step 0 is always the same: make sure  $0 \in S$ .

Step 1: Let someone choose an arbitrary element  $n$  of  $\mathbb{N}$ , then show that the statement “ $n \in S \Rightarrow s(n) \in S$ ” is true. This is the objective of Step 1, then: show that  $(\forall n \in \mathbb{N})(n \in S \Rightarrow s(n) \in S)$  is true. Since this is a statement with a universal quantifier, we have to be able to show that every one of the statements  $n \in S \Rightarrow s(n) \in S$  is true. We know by now that there is one easy way for this statement to be true: in case  $n \in S$  is false! We usually don’t mention this possibility; we just assume that  $n \in S$  is true. Then we try to use the truth of “ $n \in S$ ” to deduce the truth of “ $s(n) \in S$ .” But we can’t always work that way! Sometimes we have to use the contrapositive of “ $n \in S \Rightarrow s(n) \in S$ ,” namely “ $s(n) \notin S \Rightarrow n \notin S$ .” That is, we assume that “ $s(n) \notin S$ ” is true. Then we try to use the truth of “ $s(n) \notin S$ ” to deduce the truth of “ $n \notin S$ .” This second approach is logically equivalent to the first way, but it is not psychologically the same! Step 1 is the “heart” of an induction proof. But Step 0 is essential!

Step 3: We apply the Principle of Mathematical Induction by noting that  $S = \mathbb{N}$ . This step is one we do automatically; it’s like a coda in a piece of music. . . **end of this digression**

(04) **Example:** Let’s prove that  $s(\mathbb{N}) = \mathbb{P}$ . We need to recall that  $\mathbb{P} = \mathbb{N} \setminus \{0\}$ . We want to show that every  $n$  in  $\mathbb{P}$  is  $s(m)$  for some  $m$  in  $\mathbb{N}$ . By Postulate (01C) we know that  $(\forall n \in \mathbb{N})(s(n) \neq 0)$  is true. Thus  $s(\mathbb{N}) \subseteq \mathbb{N} \setminus \{0\} = \mathbb{P}$ . To show equality, it remains to show that  $\mathbb{P} \subseteq s(\mathbb{N})$ . We do already know of one element of  $\mathbb{P}$  that is in  $s(\mathbb{N})$ , namely  $1 = s(0)$ . Thus  $1 \in \{n \in \mathbb{P} : \text{there exists } m \in \mathbb{N} \text{ such that } n = s(m)\} =: E$ . We will use induction for  $\mathbb{P}$  instead of  $\mathbb{N}$ . We already did Step 0 (or ought it be Step 1, for  $\mathbb{P}$ ?)! We need to show that, for all  $n$  in  $\mathbb{P}$ , “ $n \in E \Rightarrow s(n) \in E$ ” is true. Well, “ $n \in E \Rightarrow s(n) \in E$ ” is true if “ $n \in E$ ” is false. Since “ $n \in E$ ” has to be true or false, we have to see what happens if “ $n \in E$ ” is true. So, we next suppose that “ $n \in E$ ” is true. Now, “ $n \in E$ ” means that there exists  $m \in \mathbb{N}$  such that  $n = s(m)$ . But then,  $s(n) = s(s(m))$ , by the Substitution Rule. The criterion for membership of  $s(n)$  in  $E$  is that there exists  $m \in \mathbb{N}$  such that  $s(n) = s(m)$ . This is confusing at first, because we just saw that  $n = s(m)$  because  $n \in E$ . The important thing to learn here is that **variables in quantifiers are “dummy” variables; we can use any convenient letter to denote them!** In the present context, we just use “ $s(m)$ ” as our convenient “letter!” Thus,  $s(n) \in E$ . Then, by Mathematical Induction (set version, for  $\mathbb{P}$ ),  $E = \mathbb{P}$ . In other words, every  $n$  in  $\mathbb{P}$  is the successor of some  $m$  in  $\mathbb{N}$ , as desired.

If you have time, I recommend that you read (listed as [3] in the References at the end of this Note) *Foundations of Analysis*, by Edmund Landau, Chelsea Publishing Co., New York, 1951. Despite the author’s request, do read the preface for the teacher. Read the preface for the student too, and the book too, a little bit at a time. What Landau does is to carefully develop the properties of the positive integers from the axioms (the version for  $\mathbb{P}$ ). Here are some exercises, adapted from theorems in that book. In these exercises, do not use your prior knowledge, just use the axioms.

(05) **Exercise:** Show that, for all  $n$  in  $\mathbb{N}$ , and for all  $m$  in  $\mathbb{N}$ , if  $n \neq m$  then  $s(n) \neq s(m)$ .

(06) **Problem:** Show that, for all  $n$  in  $\mathbb{N}$ ,  $s(n) \neq n$ . You will need induction!

(07) **Exercise:** Show that, for all  $n$  in  $\mathbb{N}$ , if  $n \neq 0$  then there exists exactly one  $m$  in  $\mathbb{N}$  such that  $n = s(m)$ . You *may* need induction!

(08) **Notation:** If  $n \in \mathbb{N}$  and  $n \neq 0$  we let  $n - 1$  denote the unique  $m$  in  $\mathbb{N}$  (provided by **Exercise** (07)) such that  $n = s(m)$ . That is,  $n = s(n - 1)$ . An important point:  $n - 1$  does not exist for all  $n$  in  $\mathbb{N}$ ;  $n - 1$  exists only for  $n \neq 0$ . This is not subtraction! The meaning of  $n - 1$  is “predecessor of  $n$ .”

**The Recursion Theorem: what justifies “definition by induction”**

**Introduction (may be skipped)** The Recursion Theorem is an Existence and Uniqueness Theorem. It asserts the existence of a certain kind of function with domain  $\mathbb{N}$  (or  $\mathbb{P}$ ) and *any* specified non-empty range space  $X$ . First, a premature definition: a *sequence* is a function whose domain is  $\mathbb{P}$  (or  $\mathbb{N}$ , if desired) and whose range space

is any non-empty set, say  $X$ . That is, a function  $f : \mathbb{N} \rightarrow X$  is called a sequence. Usually, we write  $f_n$  instead of  $f(n)$  to denote the value of  $f$  at the argument  $n$ .

Let's look at another unofficial example: Let  $x_1 := 1$ , and decree that for each  $n \geq 1$ ,  $x_{n+1} = \frac{1}{2} \left( \frac{2}{x_n} + x_n \right)$ .

This is a "definition by induction." If you are bothered by this, you are absolutely right! Does this process *really* define a sequence? The answer is that it does, but a Theorem is needed to connect  $\mathbb{N}$  and the set theory that is needed to define functions.

We defined a function to be a set of ordered pairs. The ordered pairs here are not actually specified, as they are in the definition  $F_n := \frac{n(n+1)}{2}$ . The Recursion Theorem justifies this definition.

**(09) The Recursion Theorem** *Let  $X$  be a non-empty set, and suppose that  $x_0 \in X$ . Suppose also that  $H : X \rightarrow X$  is a function. Then there exists a unique function  $R : \mathbb{N} \rightarrow X$  such that  $R(0) = x_0$  and such that for all  $n \in \mathbb{N}$ ,  $R(s(n)) = H(R(n))$ .*

**Remarks:** The first version of the proof to follow is very leisurely. It is based on the proof given in the book [2], *Naive Set Theory*, by Paul Halmos. A shorter version will follow. You might want to go directly to the short version! In the statement of the Theorem we could have written  $x_n := R(n)$ , and this would give us " $x_0$  is given, and for each  $n$ ,  $x_{s(n)} = H(x_n)$ ." The Recursion Theorem (stated for  $\mathbb{P}$  instead of  $\mathbb{N}$ ) justifies the definition of the sequence given in the Introduction:  $X$  can be the set of positive real numbers, with  $x_0 = 1$  and  $H(x) = \frac{1}{2} \left( \frac{2}{x} + x \right)$ .

*Proof of existence:* Our objective is to construct a set of ordered pairs that has the properties of a function  $H : \mathbb{N} \rightarrow X$ . We will begin by using set-selector notation to select unimaginably many sets of ordered pairs! We will define a set  $\mathcal{F}_0$  of subsets of  $\mathbb{N} \times X$ . We often use synonyms, such as "family," for the word "set" in this context so we won't have to say things like "let  $\mathcal{F}_0$  be the following set of sets..." We define the family  $\mathcal{F}_0 \subseteq 2^{\mathbb{N} \times X}$  by

$$\mathcal{F}_0 := \{S \in 2^{\mathbb{N} \times X} : (0, x_0) \in S \text{ and } (\forall n \in \mathbb{N})(\forall x \in X)((n, x) \in S \Rightarrow (s(n), H(x)) \in S)\}.$$

In words,  $\mathcal{F}_0$  is the family of all sets  $S$  of ordered pairs in  $\mathbb{N} \times X$  such that  $(0, x_0) \in S$  and, whenever  $(n, x) \in S$ , then  $(s(n), H(x)) \in S$  as well. Since  $\mathbb{N} \times X$  contains all possible ordered pairs of natural numbers  $n$  and elements  $x$  of  $X$ ,  $\mathbb{N} \times X \in \mathcal{F}_0$ . Thus  $\mathcal{F}_0$  is a non-empty family of non-empty sets.

The set  $R$  of ordered pairs we want is the set of all ordered pairs that are in every one of the sets  $S \in \mathcal{F}_0$ . Before we form this set, let's check that it can "act" like a function. We define

$$E_0 := \{n \in \mathbb{N} : \text{there exists } x \in X \text{ such that } (n, x) \in S \text{ for all } S \in \mathcal{F}_0\}.$$

Let us show that every natural number  $n$  is in  $E_0$ . This will show that when we form the set  $R$  of all ordered pairs in  $\mathbb{N} \times X$  that are in every  $S \in \mathcal{F}_0$  (we have a notation for this:  $R = \bigcap_{S \in \mathcal{F}_0} S$ ), it will be true that for every  $n \in \mathbb{N}$  there exists  $x \in X$  such that  $(n, x) \in R$ . This is one of the requirements  $R$  must satisfy if  $R$  is to be a function from  $\mathbb{N}$  to  $X$ .

*Proof that  $E_0 = \mathbb{N}$ :* We will use induction. By definition,  $(0, x_0) \in S$  for every  $S \in \mathcal{F}_0$ . Thus  $0 \in E_0$ . Now we suppose that  $n \in E_0$ . This means that there is some  $x \in X$  such that  $(n, x)$  belongs to every  $S \in \mathcal{F}_0$ . But  $(n, x) \in S \in \mathcal{F}_0$  means that  $(s(n), H(x)) \in S \in \mathcal{F}_0$ . Therefore, for every  $S \in \mathcal{F}_0$ ,  $(s(n), H(x)) \in S$ , so  $s(n) \in E_0$ . But then  $E_0$  satisfies the conditions in the Induction Axiom, so  $E_0 = \mathbb{N}$ .

Now we officially define the set  $R$ :

$$R := \bigcap_{S \in \mathcal{F}_0} S, \text{ the set of all ordered pairs } (n, x) \text{ that are in every } S \in \mathcal{F}_0.$$

**(10) Exercise:** Prove that  $R \in \mathcal{F}_0$ .

**(11) Exercise:** Prove that  $R$  is the smallest set in  $\mathcal{F}_0$ .

To prove that  $R$  is (the graph of) a function with domain  $\mathbb{N}$  and range  $X$ , we have to verify two things:

- (i) For every  $n \in \mathbb{N}$  there exists  $x \in X$  such that  $(n, x) \in R$ ;
- (ii) For all  $n$  in  $\mathbb{N}$  and all  $x_1$  and  $x_2$  in  $X$ , if  $(n, x_1) \in R$  and  $(n, x_2) \in R$  then  $x_1 = x_2$ .

We already showed that (i) is true for  $R$ , because for every  $n \in \mathbb{N}$ , there is an  $x \in X$  such that  $(n, x) \in S$  for every  $S \in \mathcal{F}_0$ . Therefore  $(n, x) \in R$ .

To verify (ii) we might begin by supposing that  $(n, x_1) \in R$  and  $(n, x_2) \in R$ . We would then have to show that  $x_1 = x_2$ . We will do this, but by induction. We define

$$E_1 := \{n \in \mathbb{N} : (\forall x_1 \in X)(\forall x_2 \in X)[(n, x_1) \in R \wedge (n, x_2) \in R] \Rightarrow [x_1 = x_2]\}.$$

If we can show that  $E_1 = \mathbb{N}$ , this will show, for arbitrary  $n \in \mathbb{N}$  and arbitrary  $x_1$  and  $x_2$  in  $X$ , that whenever  $(n, x_1) \in R$  and  $(n, x_2) \in R$  then  $x_1 = x_2$ .

*Proof that  $E_1 = \mathbb{N}$ :* We will use this idea: assume the contrary, and then construct sets in  $\mathcal{F}_0$  that are *strictly smaller* than  $R$ . Since  $R$  is the smallest set in  $\mathcal{F}_0$ , this will give the desired contradictions.

By construction,  $(0, x_0) \in R$ . If also  $(0, y_0) \in R$  and  $y_0 \neq x_0$ , we construct a new set  $S' := R \setminus \{(0, y_0)\}$ . This set has to be in  $\mathcal{F}_0$ . Firstly,  $(0, x_0) \in R$ , and, since  $x_0 \neq y_0$ ,  $(0, x_0) \in R \setminus \{(0, y_0)\} = S'$ . Secondly, if  $(m, x) \in S'$  then  $(m, x) \in R$ , so  $(s(m), H(x)) \in R$ . Moreover,  $(s(m), H(x)) \neq (0, y_0)$  because  $s(m) \neq 0$  for any  $m$ , and for ordered pairs to be unequal it's enough if one pair of two corresponding coordinates is unequal. Therefore  $(s(m), H(x)) \in R \setminus \{(0, y_0)\} = S'$ . Therefore  $S' \in \mathcal{F}_0$ . But  $S'$  is  $R$  with one element removed, so  $S'$  is strictly smaller than the smallest set in  $\mathcal{F}_0$ . This is a contradiction, so  $0 \in E_1$ .

We assume  $n \in E_1$ , and seek to show that this implies  $s(n) \in E_1$ . Again we proceed by contradiction, assuming that  $s(n) \notin E_1$ . Since  $n \in E_1$ ,  $(n, x) \in R$  for a *unique*  $x \in X$ . Then  $(s(n), H(x)) \in R$ . However, by our assumption of the contrary, there is also some  $y_1 \in X$  such that  $y_1 \neq H(x)$  and  $(s(n), y_1) \in R$  as well. We construct another set,  $S'' := R \setminus \{(s(n), y_1)\}$ .

Our strategy again is to show that  $S'' \in \mathcal{F}_0$ . As before, this will give a contradiction.

Once again,  $(0, x_0) \in S''$  because  $0 \neq s(n)$  for any natural number means that  $(0, x_0) \neq (s(n), y_1)$ .

Now we suppose that  $(m, y) \in S''$ . There are two cases to consider:  $m \neq n$  and  $m = n$ .

If  $m \neq n$ , we have  $s(m) \neq s(n)$ , so  $(s(m), H(y)) \neq (s(n), y_1)$ .

However,  $(s(m), H(y)) \in R$  because  $(m, y) \in S'' \subseteq R$ .

And  $(s(m), H(y)) \neq (s(n), y_1)$ , so  $(s(m), H(y)) \in R \setminus \{(s(n), y_1)\} = S''$ .

That is, when  $m \neq n$ ,  $(m, y) \in S'' \Rightarrow (s(m), H(y)) \in S''$ .

Finally we have to deal with the case  $m = n$ . Here,  $(m, y) = (n, y) \in R$ , so  $y = x$  (by uniqueness, because  $n \in E_1$ ) and therefore  $(s(m), H(y)) = (s(n), H(x)) \in R$ . Since  $y_1 \neq H(x)$ ,  $(s(m), H(y)) = (s(n), H(x)) \neq (s(n), y_1)$ . Hence  $(s(m), H(y)) = (s(n), H(x)) \in S''$ .

Thus  $S'' \in \mathcal{F}_0$ , which gives a contradiction. Thus  $s(n) \in E_1$ , so  $E_1 = \mathbb{N}$ . Hence (ii) is true for  $R$  so  $R$  is a function.

*Proof of uniqueness:* Suppose  $R$  and  $R'$  satisfy the conditions of the Theorem. That is,  $R(0) = x_0 = R'(0)$  and for all  $n \in \mathbb{N}$ ,  $R(s(n)) = H(R(n))$  and  $R'(s(n)) = H(R'(n))$ . We define the set

$$E_2 := \{n \in \mathbb{N} : R(n) = R'(n)\}.$$

To show that  $R' = R$  all we have to do is show that  $E_2 = \mathbb{N}$ . We use induction. We are given that  $0 \in E_2$ . If  $n \in E_2$ , then  $R'(n) = R(n)$ . But then  $R'(s(n)) = H(R'(n)) = H(R(n)) = R(s(n))$ . The second equality is by Substitution. The first and third equalities are given. Thus  $s(n) \in E_2$ , so  $E_2 = \mathbb{N}$  and so  $R' = R$ .

**A shorter version of the proof** We define the family  $\mathcal{F}_0 \subseteq 2^{\mathbb{N} \times X}$  by

$$\mathcal{F}_0 := \{S \subseteq 2^{\mathbb{N} \times X} : (0, x_0) \in S \text{ and } (\forall n \in \mathbb{N})(\forall x \in X)((n, x) \in S \Rightarrow (s(n), H(x)) \in S)\}.$$

In words,  $\mathcal{F}_0$  is the family of all sets  $S$  of ordered pairs in  $\mathbb{N} \times X$  such that  $(0, x_0) \in S$  and, whenever  $(n, x) \in S$ , then  $(s(n), H(x)) \in S$  as well. Since  $\mathbb{N} \times X$  contains all possible ordered pairs of natural numbers  $n$  and elements  $x$  of  $X$ ,  $\mathbb{N} \times X \in \mathcal{F}_0$ .

The set  $R$  of ordered pairs we want is the set of all ordered pairs that are in every one of the sets  $S \in \mathcal{F}_0$ :

$$R := \bigcap_{S \in \mathcal{F}_0} S, \text{ the set of all ordered pairs } (n, x) \text{ that are in every } S \in \mathcal{F}_0.$$

To prove that  $R$  is (the graph of) a function with domain  $\mathbb{N}$  and range  $X$ , we have to verify two things:

- (i) For every  $n \in \mathbb{N}$  there exists  $x \in X$  such that  $(n, x) \in R$ ;
- (ii) For all  $n$  in  $\mathbb{N}$  and all  $x_1$  and  $x_2$  in  $X$ , if  $(n, x_1) \in R$  and  $(n, x_2) \in R$  then  $x_1 = x_2$ .

To verify (i) we define

$$E_0 := \{n \in \mathbb{N} : \text{there exists } x \in X \text{ such that } (n, x) \in S \text{ for all } S \in \mathcal{F}_0\}.$$

Let us show that every natural number  $n$  is in  $E_0$ . We will use induction. By definition,  $(0, x_0) \in S$  for every  $S \in \mathcal{F}_0$ . Thus  $0 \in E_0$ . Next we suppose that  $n \in E_0$ . Now  $(n, x) \in S \in \mathcal{F}_0$  means that  $(s(n), H(x)) \in S \in \mathcal{F}_0$ . Therefore, for every  $S \in \mathcal{F}_0$ ,  $(s(n), H(x)) \in S$ , so  $s(n) \in E_0$ . But then  $E_0$  satisfies the conditions in the Induction Axiom, so  $E_0 = \mathbb{N}$  and thus (i) is true for  $R$ .

To verify (ii) we define

$$E_1 := \{n \in \mathbb{N} : (\forall x_1 \in X)(\forall x_2 \in X)[((n, x_1) \in R \wedge (n, x_2) \in R) \Rightarrow [x_1 = x_2]]\}.$$

If we can show that  $E_1 = \mathbb{N}$ , this will show, for arbitrary  $n \in \mathbb{N}$  and arbitrary  $x_1$  and  $x_2$  in  $X$ , that whenever  $(n, x_1) \in R$  and  $(n, x_2) \in R$  then  $x_1 = x_2$ .

*Proof that  $E_1 = \mathbb{N}$ :* We will use this idea: assume the contrary, and then construct sets in  $\mathcal{F}_0$  that are *strictly smaller* than  $R$ . Since  $R$  is the smallest set in  $\mathcal{F}_0$ , this will give the desired contradictions.

By construction,  $(0, x_0) \in R$ . If also  $(0, y_0) \in R$  and  $y_0 \neq x_0$ , we construct  $S' := R \setminus \{(0, y_0)\}$ . We show  $S' \in \mathcal{F}_0$ . Firstly,  $(0, x_0) \in R$ , and, since  $x_0 \neq y_0$ ,  $(0, x_0) \in R \setminus \{(0, y_0)\} = S'$ . Secondly, if  $(m, x) \in S'$  then  $(m, x) \in R$ , so  $(s(m), H(x)) \in R$ . Moreover,  $(s(m), H(x)) \neq (0, y_0)$  because  $s(m) \neq 0$  for any  $m$ . Therefore  $(s(m), H(x)) \in R \setminus \{(0, y_0)\} = S'$ . Therefore  $S' \in \mathcal{F}_0$ . But  $S'$  is strictly smaller than  $R$ , the smallest set in  $\mathcal{F}_0$ . This is a contradiction, so  $0 \in E_1$ .

We assume  $n \in E_1$ , and seek to show that this implies  $s(n) \in E_1$ . Again we proceed by contradiction, assuming that  $s(n) \notin E_1$ . Since  $n \in E_1$ ,  $(n, x) \in R$  for a *unique*  $x \in X$ . Then  $(s(n), H(x)) \in R$ . However, by our assumption of the contrary, there is also some  $y_1 \in X$  such that  $y_1 \neq H(x)$  and  $(s(n), y_1) \in R$  as well. We construct another set,  $S'' := R \setminus \{(s(n), y_1)\}$ .

Our strategy again is to show that  $S'' \in \mathcal{F}_0$ . As before, this will give a contradiction. Since  $0 \neq s(n)$  for any natural number,  $(0, x_0) \in S''$ .

We suppose  $(m, y) \in S''$  and consider two cases:  $m \neq n$  and  $m = n$ .

If  $m \neq n$ ,  $s(m) \neq s(n)$ , so  $(s(m), H(y)) \neq (s(n), y_1)$ .

As  $(s(m), H(y)) \neq (s(n), y_1)$ ,  $(s(m), H(y)) \in R \setminus \{(s(n), y_1)\} = S''$ .

That is, when  $m \neq n$ ,  $(m, y) \in S'' \Rightarrow (s(m), H(y)) \in S''$ .

If  $m = n$ ,  $(m, y) = (n, y)$  so  $y = x$  and therefore  $(s(m), H(y)) = (s(n), H(x)) \in R$ . Since  $H(x) \neq y_1$ , we have  $(s(m), H(y)) \in S''$ .

Thus  $S'' \in \mathcal{F}_0$ , which gives a contradiction. Hence (ii) is true for  $R$  so  $R$  is a function.

To prove uniqueness suppose  $R$  and  $R'$  satisfy the conditions of the Theorem. We define the set

$$E_2 := \{n \in \mathbb{N} : R(n) = R'(n)\}.$$

To show that  $R' = R$  we show that  $E_2 = \mathbb{N}$ . We use induction. We are given that  $0 \in E_2$ . If  $n \in E_2$ , then  $R'(n) = R(n)$ . But then  $R'(s(n)) = H(R'(n)) = H(R(n)) = R(s(n))$ . Thus  $s(n) \in E_2$ , so  $E_2 = \mathbb{N}$  and so  $R' = R$ .

**The construction of the operation of addition** All we have now is the Peano Axioms and the Recursion Theorem! Addition and multiplication are not in the Axioms, so they have to be re-built!

Theorem 4 in Landau's book [3] is also a definition, that of addition, defined in terms of the successor function. This theorem is mentioned as part of an interesting "confession" in the preface to the teacher. The proof in [3] is hard to follow. Here is the Theorem, paraphrased to fit  $\mathbb{N}$  instead of  $\mathbb{P}$ .

**(12) Theorem and Definition (of) and notation (for) ([on] addition):**

There exists one and only one function  $p : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  with the following properties ( $p$  is for "plus"):

(A) for all  $n$  in  $\mathbb{N}$ ,  $p(n, 0) = n$ ;

(B) for all  $n$  in  $\mathbb{N}$ , and for all  $m$  in  $\mathbb{N}$ ,  $s(p(n, m)) = p(n, s(m))$ .

We call finding the value of  $p(n, m)$  addition of  $n$  and  $m$ , and we call the value of  $p(n, m)$  the sum of  $n$  and  $m$ . We use the notation  $n + m := p(n, m)$ .

The ordered pairs that comprise the function  $p$  have first members that are themselves ordered pairs! For example,  $((1, 0), 1)$  and  $((1, 1), 2)$  are "in"  $p$ . They correspond to  $1 + 0 = 1$  and to  $1 + 1 = 2$ , respectively. Landau proves this Theorem in two main steps. First, he shows that there is at most one function that has properties (A) and (B). This is the "only one" part of the proof; this may strike you as odd, because we don't know yet whether there is any such function! The point is that we assume there are two such functions, and then show they must be equal functions! This is the standard way to approach a proof of uniqueness: assume there are two objects with all the properties under study, and then show that the two objects must be equal to each other.

*Proof:* (Uniqueness part)

Suppose that  $p$  and  $q$  are two functions that satisfy (A) and (B). We will show that, for each  $n_o$  in  $\mathbb{N}$ , given and fixed,  $p(n_o, m) = q(n_o, m)$  for all  $m$  in  $\mathbb{N}$ . I'm often going to write "for all  $m$ " as a short version of "for all  $m$  in  $\mathbb{N}$ ." We will use Mathematical Induction (the set version). We'll define a set  $S$  that consists of all the  $m$ 's such that  $p(n_o, m) = q(n_o, m)$ . Then we'll set out to show, using Mathematical Induction, that  $S = \mathbb{N}$ . This will show that  $p(n_o, m) = q(n_o, m)$  for all  $m$ . But then, since  $n_o$  was arbitrary, it'll also be true that for all  $n$ ,  $p(n, m) = q(n, m)$  for all  $m$ . This is what we mean by equality of functions of two variables. Now, let's do the proof!

Let  $S$  denote the set of all  $m$  such that  $p(n_o, m) = q(n_o, m)$ .

In set selector notation,  $S := \{m \in \mathbb{N} : p(n_o, m) = q(n_o, m)\}$ . Let us show that 0 is in  $S$ . By (A),  $p(n, 0) = n$  for all  $n$ , and by (A),  $q(n, 0) = n$  for all  $n$ . Thus, for our fixed  $n$ , namely  $n_o$ , we have  $p(n_o, 0) = q(n_o, 0)$ . This means that 0 is in  $S$ . Now suppose that  $m$  is in  $S$  (that is,  $m$  is the name of an element in  $S$ ; we don't know which  $m$ ). Membership of  $m$  in  $S$  means that  $p(n_o, m) = q(n_o, m)$ . We want to show that  $s(m)$  is in  $S$ . This means we have to show that  $p(n_o, s(m)) = q(n_o, s(m))$ . Since  $p(n_o, m) = q(n_o, m)$ ,

$$(12-1) \quad s(p(n_o, m)) = s(q(n_o, m)), \text{ using Substitution.}$$

We choose, as the values of the variables  $n$  and  $m$  in (B),  $n_o$  and the particular  $m$  that we assumed was in  $S$ . Then by (B), the Reflexivity of Equality, (9-1) and (B) again,

$$p(n_o, s(m)) = s(p(n_o, m)) = s(q(n_o, m)) = q(n_o, s(m)).$$

Therefore, by the Transitivity of Equality,  $p(n_o, s(m)) = q(n_o, s(m))$ . By the definition of  $S$ ,  $s(m)$  thus belongs to  $S$  if  $m$  does. Hence  $S = \mathbb{N}$ , by the Principle of Mathematical Induction.

This means that for  $n_o$ ,  $p(n_o, m) = q(n_o, m)$  for all  $m$ . But our fixed  $n$ ,  $n_o$ , was any  $n_o$  at all. That is, for all  $n$ ,  $p(n, m) = q(n, m)$  for all  $m$ . This is the condition for equality of functions with two variables: for all  $n$  and  $m$ ,  $p(n, m) = q(n, m)$ . That is,  $p = q$ . **We use a completely arbitrary element  $n_o$  of  $\mathbb{N}$  to prove a "for all" statement!**

The uniqueness part is done: if there is a function that works, there is only one!

*Proof:* (Existence part) This is where we show that yes, there *IS* a function that works! In Spring Semester 2002, Leonard Blackburn, who was one of the Teaching Assistants, after students Brian Lucore and Karen Speltz talked to him, found and pointed out a flaw in the proof in an earlier version of these notes, based on what Landau supplied to deal with the difficulty discussed in the Preface for the Teacher in [3]! Nevertheless I recommend reading Landau's book, a truly valuable contribution!

Here is our attempt to make a correct version of Landau's proof, using the Recursion Theorem. This will make the proof longer than it needs to be, for Mr. Blackburn [1] has a much shorter one, that also uses the Recursion Theorem. You might well prefer to look at the two proofs given by Mr. Blackburn in [1], pages 5 and 6. Their *combined* length is much shorter than the proof given here!

To prove that the function  $p$  exists, we are seeking to prove that a function of two variables exists. To make this look a little better let's think instead about defining a sequence of functions of one variable:  $p_n(m) := p(n, m)$ . We then need to translate what we want (namely (A) and (B) in the statement of the Theorem) into these terms:

$$\begin{aligned} (A') & \text{ for all } n \text{ in } \mathbb{N}, p_n(0) = n; \\ (B') & \text{ for all } n \text{ in } \mathbb{N}, \text{ and for all } m \text{ in } \mathbb{N}, s(p_n(m)) = p_n(s(m)). \end{aligned}$$

In these new terms, we see that we want each function  $p_n$  to "commute" with the successor function! That is, in terms of "function notation,"  $s \circ p_n = p_n \circ s$ , as functions from  $\mathbb{N}$  to  $\mathbb{N}$ .

Let us "construct" a function  $p_0$  to start the process.

Since we are going to "create" something, we duck into the "back room" and use our knowledge, especially the things we take for granted. We want  $p(n, m) = n + m$ . We really don't know how to define addition "in one jump," but we do know that  $0 + m$  "ought" to be  $m$ . So we "construct" or **define**  $p_0(m) := m$  for all  $m \in \mathbb{N}$ . We emerge from the "back room" and continue.

Let  $p_0(m) := m$  for all  $m$ . So  $p_0$  exists. We now show that  $p_0$  satisfies conditions (A') and (B') when  $n = 0$ . For (A') we need  $p_0(0) = 0$ , which is true by our definition of  $p_0$ . For (B') we need: for all  $m$  in  $\mathbb{N}$ ,  $s(p_0(m)) = p_0(s(m))$ . By Substitution,  $s(p_0(m)) = s(m)$ . Since  $p_0$  "sends" each element of  $\mathbb{N}$  to itself,  $p_0(s(m)) = s(m)$ . By Transitivity of Equality,  $s(p_0(m)) = p_0(s(m))$ .

Next we use the Recursion Theorem to produce the rest of the functions  $p_n$ . This requires some big thinking! We will use the "subscripted" version of the Recursion Theorem, mentioned in the Remarks following the Recursion Theorem's statement. We will select as our set  $X$  the set of all functions from  $\mathbb{N}$  to  $\mathbb{N}$ , usually denoted as  $X = \mathbb{N}^{\mathbb{N}}$ . Our  $x_0$  is the function  $p_0$  that we just constructed. We need a function  $H : X \rightarrow X$ . We will use composition with the successor function. That is, if  $p : \mathbb{N} \rightarrow \mathbb{N}$ , then  $H(p)$  is the function defined by the rule  $H(p)(m) := s(p(m))$  for all  $m \in \mathbb{N}$ . Or,  $H(p) := s \circ p$ . According to the Recursion Theorem, there is a unique function  $R : \mathbb{N} \rightarrow X$  such that  $R_0 = p_0$  and, for all  $n \in \mathbb{N}$ ,  $R_{s(n)} = H(R_n)$ . Let us decipher what we have done! First, we have  $R_n : \mathbb{N} \rightarrow \mathbb{N}$ . That is, for each  $m \in \mathbb{N}$ ,  $R_n(m) \in \mathbb{N}$ . Therefore the statement  $R_{s(n)} = H(R_n)$  means that

$$(12-2) \quad \text{for all } m \in \mathbb{N}, R_{s(n)}(m) = H(R_n)(m) = s(R_n(m)).$$

We can ask, what is  $R_n(0)$ ? We hope that  $R_n$  will be our  $p_n$ , so we want  $R_n(0) = n$ . Let us prove by induction that  $R_n(0) = n$  for all  $n \in \mathbb{N}$ . We have  $R_0(0) = p_0(0) = 0$ , so  $0 \in \{m \in \mathbb{N} : R_m(0) = m\}$ . If  $n \in \{m \in \mathbb{N} : R_m(0) = m\}$ , then by the Recursion Theorem,  $R_{s(n)}(0) = s(R_n(0)) = s(n)$ , so  $s(n) \in \{m \in \mathbb{N} : R_m(0) = m\}$ , and then by Induction,  $\{m \in \mathbb{N} : R_m(0) = m\} = \mathbb{N}$ . In other words, (A') is true for the functions  $R_n$ . We next want to show that (B') is true for the functions  $R_n$ , namely that for all  $n$  in  $\mathbb{N}$ , and for all  $m$  in  $\mathbb{N}$ ,  $s(R_n(m)) = R_n(s(m))$ .

We let

$$E := \{n \in \mathbb{N} : \text{for all } m \in \mathbb{N}, s(R_n(m)) = R_n(s(m))\}.$$

We will use the Principle of Mathematical Induction to show that  $E = \mathbb{N}$ . The first step is to show that  $0$  is in  $E$ . When  $n = 0$  we are to show that  $s(R_0(m)) = R_0(s(m))$  for all  $m \in \mathbb{N}$ . We know this is true, since  $R_0 = p_0$ , and we have shown this to be true for  $p_0$ . Thus  $0 \in E$ .

Next we assume  $n \in E$ , so that for all  $m \in \mathbb{N}$ ,  $s(R_n(m)) = R_n(s(m))$ . We want to show that, because of this, for all  $m \in \mathbb{N}$ ,  $s(R_{s(n)}(m)) = R_{s(n)}(s(m))$ . We will show, for an arbitrary  $m \in \mathbb{N}$ , that the two sides of this

equation are equal to the same thing. Transitivity of Equality will then give us what we need. The term on the left is  $s(R_{s(n)}(m)) = s(s(R_n(m)))$  by (12-2), applied to the quantity “inside” the  $s$ . The term on the right is, again by (12-2),

$$(12-3) \quad R_{s(n)}(s(m)) = s(R_n(s(m))).$$

Now we use the assumption that  $n \in E$ , which assured us that for all  $m \in \mathbb{N}$ ,  $s(R_n(m)) = R_n(s(m))$ . We may (and do!) replace the  $R_n(s(m))$  “inside” the  $s$  on the right in (9-3) by  $s(R_n(m))$ , so that

$$R_{s(n)}(s(m)) = s(s(R_n(m))).$$

Thus  $s(R_{s(n)}(m)) = s(s(R_n(m))) = R_{s(n)}(s(m))$ , as desired, so  $E = \mathbb{N}$ . We only have to rename our  $R_n$ :  $p_n := R_n$ , and we have functions  $p_n$  that satisfy the conditions (A') and (B').

Now we just define  $p(n, m) := p_n(m)$ . You are now asked to complete the proof by working the following exercise.

(13) **Exercise:** Show that  $p(n, m)$  satisfies the conditions in the Theorem.

Do you agree that the proof was difficult to follow? There is more difficulty to come! We are now beginning to rebuild the basic arithmetic operations you learned how to do in grade school. Now you are moving toward understanding what numbers mean, and how the operations “work.” I concede the operations don’t work, you do!

(14) **Exercise:** Show that, for all  $n$ ,  $s(n) = n + s(0)$  [=  $p(n, s(0))$ ]. We now define  $1 := s(0)$ . You are thus showing  $s(n) = n + 1$ : hence the name “successor” for the function  $s$ .

(15) **Problem:** Define  $2 := s(1)$ , and  $3 := s(2)$ , and  $4 := s(3)$ . Show that  $2 + 2 = 4$ . You will probably need to look in the proof of the theorem about addition.

The preceding theorem and its proof show how Landau constructed addition. He did not use the Recursion Theorem, instead using a consequence of it that he did not prove.

(16) **Problem:** Show:  $(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(\forall r \in \mathbb{N})(p + (q + r) = (p + q) + r)$ . You’ll need to fix  $p$  and  $q$ , and let  $S$  denote the set of all  $r$  such that the statement  $p + (q + r) = (p + q) + r$  is true. What is the name for what this theorem says about the operation of addition?

(17) **Exercise:** Show:  $(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(p + q = q + p)$ . You’ll need to fix  $p$ , and let  $S$  denote the set of all  $q$  such that the statement  $p + q = q + p$  is true. This Theorem is called the \_\_\_\_\_ Law of Addition.

(18) **Problem:** Show:  $(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(\forall r \in \mathbb{N})(\text{If } p + q = p + r \text{ then } q = r)$ . What is the name of this Theorem? Suggestion: Fix arbitrary  $q$  and  $r$  in  $\mathbb{N}$ . Consider the set  $S := \{p \in \mathbb{N} : p + q = p + r \Rightarrow q = r\}$ .

The next Theorem gives an important property of addition. The statement of the Theorem will have two Universal quantifiers and one Existential quantifier. Its proof once again uses Mathematical Induction, which we can think of as “using up” one of the Universal quantifiers.

(19) **Theorem:** For all natural numbers  $n$  and  $m$  there exists a natural number  $k$  such that  $n = m + k$  or  $m = n + k$ . (“in logic,” the theorem asserts  $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\exists k \in \mathbb{N})([n = m + k] \vee [m = n + k])$ .”)

*Proof:* We define  $E$  to be the set of all natural numbers  $n$  such that for all natural numbers  $m$  there exists a natural number  $k$  such that  $n = m + k$  or  $m = n + k$ . In set-selector notation,

$$E = \{n \in \mathbb{N} : (\forall m \in \mathbb{N})(\exists k \in \mathbb{N})([n = m + k] \vee [m = n + k])\}.$$

If we can show that  $E = \mathbb{N}$ , then  $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\exists k \in \mathbb{N})([n = m + k] \vee [m = n + k])$  is true.

**First we will show that**  $0 \in E$ . To do so we have to prove that

$$(19-1) \quad (\forall m \in \mathbb{N})(\exists k \in \mathbb{N})([0 = m + k] \vee [m = 0 + k]) \text{ is true.}$$

The “rule” for proving a statement that begins with a Universal quantifier is to allow your worst enemy (assumed not you!) to pick the worst possible value of the variable! Then you have to use that value as the variable’s value. So we say (perhaps resignedly) “Let  $m \in \mathbb{N}$  be given.” This signifies that we are working with a completely arbitrary member of  $\mathbb{N}$ . We can use about it only that which is true for every element of  $\mathbb{N}$ , which is that  $m$  is in  $\mathbb{N}$ .

Let  $m \in \mathbb{N}$  be given. If we select  $k = m$  then the statement  $m = 0 + k = k$  is true by Substitution (of  $m$  for  $k$ ). Thus  $[0 = m + k] \vee [m = 0 + k]$  is true about  $m$  and  $k$  when  $k = m$ . Since  $m$  was arbitrary, we have in effect proved that (19-1) is true by proving it for all  $m$  “simultaneously!” **Thus  $0 \in E$  has been shown.**

Next, we assume that  $n \in E$  and seek to prove that  $n + 1 = s(n) \in E$ . **Since  $n$  has now been specified, let us call  $n$  by the name  $n_o$ , to remind us that  $n$  is not a variable any more, but is now a “constant.”** We are given that

$$(19-2) \quad (\forall m \in \mathbb{N})(\exists k \in \mathbb{N})( [n_o = m + k] \vee [m = n_o + k] ) \text{ is true.}$$

We seek to prove that

$$(19-3) \quad (\forall m \in \mathbb{N})(\exists k \in \mathbb{N})( [n_o + 1 = m + k] \vee [m = (n_o + 1) + k] ) \text{ is true.}$$

Here we will depart from the “rule” and show first that if (19-2) is true then

$$(19-4) \quad (\exists k \in \mathbb{N})( [n_o + 1 = 0 + k] \vee [0 = (n_o + 1) + k] ) \text{ is true,}$$

which is the part of (19-3) we get when  $m = 0$ . But (19-4) becomes true if we take  $k = n_o + 1$ , so (19-4) is true.

The best “strategy” for proving a statement that begins with an Existential quantifier is to **guess** a value of the variable that we think will work and then **check** that the chosen value makes true the statement that follows the quantifier. Usually the guess is “informed” by a bit of thought and pencil-and-paper scratch work! The checking, we hope will be easy, but it too sometimes takes work.

Now to prove the “ $\forall m \in \mathbb{N}$ ” part of (19-3) we only have to prove that (19-3) is true whenever  $m \neq 0$ , because we know it’s true whenever  $m$  is 0.

Let  $0 \neq m \in \mathbb{N}$  be given. Then there exists  $k \in \mathbb{N}$  such that  $[n_o = m + k] \vee [m = n_o + k]$  is true. Now all the variables have been specified! Let us name the newly specified ones  $m_o$  and  $k_o$  respectively.

There are two cases to consider: Case 1 is “ $n_o = m_o + k_o$  is true,” Case 2 is “ $m_o = n_o + k_o$  is true,” because we do not know which of  $n_o = m_o + k_o$  and  $m_o = n_o + k_o$  is true, just that at least one of them is true.

**Case 1:**  $n_o = m_o + k_o$ , so  $n_o + 1 = (m_o + k_o) + 1 = m_o + (k_o + 1)$  by **Problem** (13). That is,  $n_o + 1 = m_o + (k_o + 1)$ . Thus (19-3) is true when  $m = m_o$  if we choose the  $k$  there to be  $k = k_o + 1$  (we recall that an OR statement is true if the first statement in it is true).

**Case 2:**  $m_o = n_o + k_o$ . We now have subcases! We do not know the value of  $k_o$ , but in  $\mathbb{N}$  0 is “special” so we need to consider Subcases 2a and 2b.

**Subcase 2a:**  $k_o = 0$  so  $m_o = n_o + k_o = n_o + 0 = n_o = m_o$ . Then  $n_o + 1 = m_o + 1$  by Substitution, so (19-3) is true when  $m = m_o$  if we choose the  $k$  there to be  $k = 1$ .

**Subcase 2b:**  $k_o \neq 0$ , so by **Exercise** (07) there exists  $j_o$  such that  $k_o = s(j_o) = j_o + 1$ . Then we have, by hypothesis (Case 2), by Substitution, by commutativity and associativity that

$$m_o = n_o + k_o = n_o + (j_o + 1) = n_o + (1 + j_o) = (n_o + 1) + j_o.$$

Thus (19-3) is true when  $m = m_o$  if we choose the  $k$  there to be  $k = j_o$  (we recall that an OR statement is true if the second statement in it is true). **We have proved that (19-3) is true if (19-2) is true, and the truth of (19-3) shows that  $n_o + 1$  is in  $E$ .**

By Mathematical Induction, we have shown that Theorem (19) is true, so the proof is complete. Theorem (19) will be useful when we consider properties of “ordering” in the Natural Numbers, which is our next topic.

## ORDER AND INEQUALITIES

Inequalities are very important in advanced mathematics. Next, we develop techniques for dealing with them, as we develop the properties of inequalities, or the ordering relations. Here is (in effect) how Landau defines the relation  $n \leq m$ :

(20) **Definition and notation:** Let  $n$  and  $m$  belong to  $\mathbb{N}$ . Then  $n$  is *less than or equal to*  $m$  if there exists  $k$  in  $\mathbb{N}$  such that  $n + k = m$ . We express this in symbols by writing  $n \leq m$ .

(21) **Definition and notation:** Let  $n$  and  $m$  belong to  $\mathbb{N}$ . Then  $n$  is *less than*  $m$  if there exists  $k$  in  $\mathbb{N}$  such that  $k \neq 0$  and  $n + k = m$ . We express this in symbols by writing  $n < m$ . The inequality  $n < m$  is called a *strict inequality*.

(22) **Exercise:** Show:  $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(\text{ If } n \leq m \text{ and } m \leq n \text{ then } n = m)$ . Hint: Remember that  $n + 0 = n$ .

(23) **Exercise:** Show:  $(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(\forall r \in \mathbb{N})(\text{ If } p \leq q \text{ and } q \leq r \text{ then } p \leq r)$ . What is this property of  $\leq$  called?

(24) **Exercise:** Show that, for all  $n$ ,  $n < s(n)$ .

(25) **Problem:** Show that, if  $n < m$  and  $m < p$ , then  $n < p$ . You will need to use the associativity of addition. State the problem's statement in a standard logical form. There are some missing quantifiers! What can you expect to be true, if you encounter a string of inequalities, all in the same direction, such as  $p \leq q \leq r < s$ , about the relation between  $p$  and  $s$ ?

(26) **Problem:** Show that, if  $n < m$ , then  $n + p < m + p$  for all  $p$ . You will need to use associativity and commutativity of addition. State the problem's statement in a standard logical form. There are some missing quantifiers!

(27) **Exercise:** Define  $n > m$  and  $n \geq m$ , and show that each of these relations is transitive. We will say " $n$  is larger than  $m$ " or " $n$  is greater than  $m$ ," when " $n > m$ " is true, and use similar phrases when " $n \geq m$ " is true. You will need to use associativity of addition to show transitivity.

Please notice that we have NOT shown that " $n \geq m$ " is the denial of " $n < m$ ". It is true, but has yet to be proved! You will do this later, in (30), a Special **Problem** .

(28) **Exercise:** Show that, for all  $n$ , if  $n \neq 0$ , then  $1 \leq n$ . You need to use the definition of  $1 : 1 = s(0)$ . You are also showing that there is no natural number strictly between 0 and 1! Suggestion: let  $S := \{0\} \cup \{n \in \mathbb{N} : 1 \leq n\}$ . You'll need to use transitivity of  $\leq$ .

The list of things Landau proves is long, and each thing on the list is something you have learned to take for granted. But now you are being asked to take on the task of certifying (or not!) the work of past generations to future ones!

One very important theorem Landau proves is this:

(29) **Theorem (Trichotomy Law):** For all  $n$  in  $\mathbb{N}$ , and for all  $m$  in  $\mathbb{N}$ , exactly one of the following is true:

- (1)  $n = m$ ; (2)  $n < m$ ; (3)  $m < n$ .

(30) **Special Problem:** Prove Theorem (26). You will need to use the equation that defines " $n < m$ ." You already know that  $s(n) \neq n$  and  $s(n) > n$ . It may help to prove that, "for all  $n$  in  $\mathbb{N}$ ,  $\sim (s(n) < n)$ " is true.

(31) **Theorem:**  $(\forall p \in \mathbb{N})(\forall q \in \mathbb{N})(\forall r \in \mathbb{N})(\text{ If } p + q < p + r \text{ then } q < r)$ .

*Proof:* We have to show that, for every choice of three elements  $p$ ,  $q$  and  $r$  in  $\mathbb{N}$ , the statement "If  $p + q < p + r$  then  $q < r$ " is true. The statement has the form "If  $A$  then  $B$ ." In case  $A$  is false, we don't have anything to do; the statement is vacuously true. Therefore, we will assume that  $A$  is true, and try to deduce  $B$ . We usually do this sort of thing without saying so. The way we often say that we are assuming that  $A$  is true is, in the present case: "Given:  $p + q < p + r$ ." By definition of " $<$ ," there exists  $s \neq 0$  such that  $(p + q) + s = (p + r)$ . Therefore, by associativity (see (14)), and the Transitivity of Equality,  $p + (q + s) = p + r$ . By (18), the Cancellation Law for addition,  $q + s = r$ . Since  $s \neq 0$ , this means, by definition, that  $q < r$ , as desired.

This proof is a good example of using of a definition in two ways. We are given that  $p + q < p + r$ . Then we look up the definition (or, better yet, recall it!), and translate its symbols into the context of the problem. That is why parentheses are used on both sides of the equation in the second sentence of the proof:  $p + q$  and  $p + r$  are to be thought of as single elements of  $\mathbb{N}$ . So we get, using the given truth of the definition's statement, and associativity, and cancellation, the equation  $q + s = r$ . Next we use the definition backwards! I call this a "recognition step:" We recognize that the equation  $q + s = r$ , with  $s \neq 0$ , occurs in the definition of " $q < r$ ." Since the equation is true, we then conclude that the criterion for saying " $q < r$ " is satisfied.

(32) **Definition:** If  $S$  is a set contained in  $\mathbb{N}$ ,  $S$  has a least element if there exists  $m \in S$  such that, for all  $n \in \mathbb{N}$ , if  $n \in S$ , then  $m \leq n$ .

(33) **Problem:** Write the statement of the definition in logic notation, giving careful attention to the placement of quantifiers. Be sure that no quantifiers include “ $\notin S$ .”

(34) **Exercise:** Show that, if the statement “ $S$  has a least element” is true, then there is only one  $m$  such that “ $m \in S$ , and, for all  $n \in \mathbb{N}$ , if  $n \in S$ , then  $m \leq n$ ” is true. Suggestion: This is a uniqueness theorem, so you might begin by assuming that “ $m_1 \in S$ , and, for all  $n \in \mathbb{N}$ , if  $n \in S$ , then  $m_1 \leq n$ ” is true, and “ $m_2 \in S$ , and, for all  $n \in \mathbb{N}$ , if  $n \in S$ , then  $m_2 \leq n$ ” is true, and then show that  $m_1 = m_2$ .

(35) **Definition and notation:** If  $S$  is a set contained in  $\mathbb{N}$ , and  $S$  has a least element, then, the least element of  $S$  is the unique (by (34))  $m$  in  $S$  such that, for all  $n \in \mathbb{N}$ , if  $n \in S$ , then  $m \leq n$ . We denote this unique  $m$  by  $\min(S)$ .

(36) **Exercise:** Show that 0 is the least element of  $\mathbb{N}$ , i.e., that  $0 = \min(\mathbb{N})$ .

(37) **Exercise:** Does the empty subset of  $\mathbb{N}$  have a least element? You will probably need the answer to (33) to be sure about your answer to this exercise.

(38) **Exercise:** Devise a definition of “ $S$  has a greatest element,” and of  $\max(S)$ .

### The Well-Ordering Theorem - a very powerfully applicable theorem

(39) **Theorem (Well-Ordering):** Every non-empty subset of  $\mathbb{N}$  has a least element.

*Proof:* (Note: a shorter version of the proof follows this very long one. You might want to skip to the short version now!) We will use a contradiction argument. We will do this in great detail!

Let us express the mathematical statement in the Theorem in logic notation:

$$(\forall S \in 2^{\mathbb{N}})(S \neq \emptyset \Rightarrow (\exists m \in \mathbb{N})(m \in S \wedge (\forall n \in \mathbb{N})(n \in S \Rightarrow m \leq n))).$$

To use a contradiction argument, we **ASSUME** that the denial of the desired mathematical statement is true, and we seek to **deduce**, using the assumed “truth,” a contradiction. The contradiction tells us that the statement we assumed true (namely, the denial of what we wanted to be true) is actually false. The Law of the Excluded Middle then says that  $S$  does have a least element. Thus, **let us assume the denial is true**. The denial, **now true**, of our mathematical statement is

$$(\exists S \in 2^{\mathbb{N}})(S \neq \emptyset \wedge (\forall m \in \mathbb{N})(m \notin S \vee (\exists n \in \mathbb{N})(n \in S \wedge m > n))).$$

Since this is true, we “can find” a set  $S_o$  such that

$$S_o \neq \emptyset \wedge (\forall m \in \mathbb{N})(m \notin S_o \vee (\exists n \in \mathbb{N})(n \in S_o \wedge m > n)).$$

is true. For convenience, let us write this in the equivalent form

$$S_o \neq \emptyset \wedge (\forall m \in \mathbb{N})(m \in S_o \Rightarrow (\exists n \in \mathbb{N})(n \in S_o \wedge n < m)).$$

We obtain such a set  $S_o$ , a non-empty subset of  $\mathbb{N}$ . Then each of the mathematical statements

(39-1)  $S_o \neq \emptyset$  and  $(\forall m \in \mathbb{N})(m \in S_o \Rightarrow (\exists n \in \mathbb{N})(n \in S_o \wedge n < m))$  is true.

We are not going to use the non-emptiness of  $S_o$  until the very end of the argument. We are going to show that

$$(\forall m \in \mathbb{N})(m \in S_o \Rightarrow (\exists n \in \mathbb{N})(n \in S_o \wedge n < m)) \Rightarrow S_o = \emptyset \text{ is true.}$$

Since we have already assumed that (39-1) is true, we deduce that

(39-2)  $(\forall m \in \mathbb{N})(m \in S_o \Rightarrow (\exists n \in \mathbb{N})(n \in S_o \wedge n < m))$  is true (why?).

Thus we have to deduce that  $S_o = \emptyset$  is true.

It is usually a good idea to examine a statement to see what it means, at the “work” level. Let’s do that.

Since (39-2) begins with a universal quantifier, we can choose  $m = 0$ , and deduce that

(39-3)  $0 \in S_o \Rightarrow (\exists n \in \mathbb{N})(n \in S_o \wedge n < 0)$  is true.

The reason for choosing  $m = 0$  is this: we can look at the statement (39-3) and “see” that it must be false, because  $n < 0$  must be false. But how can we *prove* that  $n < 0$  must be false (for  $n \in \mathbb{P}$ )? If  $n < 0$  were not false, there would exist  $n \in \mathbb{N}$  such that  $n < 0$ . By definition,  $n < 0$  means that there exists  $k$  in  $\mathbb{N}$  such that  $k \neq 0$  and  $0 = n + k$ . Since  $k \neq 0$ , we can apply an exercise you have done ( (07) ) that said, using the present notation, “for

all  $k$  in  $\mathbb{N}$ , if  $k \neq 0$  then there exists exactly one  $j$  in  $\mathbb{N}$  such that  $k = s(j)$ .” Now we can go back to the proof of the theorem about addition, and say  $0 = n + k = p(n, k) = p(n, s(j)) = s(p(n, j))$ . Therefore,  $0$  is the successor of  $p(n, j)$ . But  $0$  is not the successor of any element of  $\mathbb{N}$  (one of the axioms!). We have produced a contradiction of the form “ $A$  and not- $A$ .” Hence  $n < 0$  is false for all  $n$ .

How does all this help us? We wanted to show that  $0 \notin S_o$ . We have deduced that (39-3) is true, and we have shown that  $(\exists n \in \mathbb{N})(n \in S_o \wedge n < 0)$  is false.

The true mathematical statement (39-3) has the logical form  $A \Rightarrow B$ ,  
with  $A = “0 \in S_o”$  and  $B = “(\exists n \in \mathbb{N})(n \in S_o \wedge n < 0)”$ .

Since  $B$  is false, that is,  $\sim B$  is true, we can deduce that  $\sim A$  is true, namely, that  $A$  is false. Why?

Therefore, we have deduced that “ $0 \in S_o$ ” is false, so  $0 \notin S_o$ , as desired.

What have we done so far? We have shown that, if a non-empty subset of  $\mathbb{N}$  does not have a least element, then it cannot contain  $0$ . You could, if you wished, use the same idea show that it cannot contain  $1$  either. What we want to do is to show that it cannot contain *any* natural number. This is where we will get the desired contradiction to use in proving the whole theorem.

Let us look again at the mathematical statement (39-1):

$$S_o \neq \emptyset \wedge (\forall m \in \mathbb{N})(m \in S_o \Rightarrow (\exists n \in \mathbb{N})(n \in S_o \wedge n < m)).$$

We have deduced from it that  $0 \notin S_o$ . We did it by showing that  $(\exists n \in \mathbb{N})(n \in S_o \wedge n < 0)$  is false. We would like to show that, for *all*  $m$  in  $\mathbb{N}$ ,  $m \in S_o$  is false.

Here is an **idea**: show that, for all  $m$  in  $\mathbb{N}$ ,  $(\exists n \in \mathbb{N})(n \in S_o \wedge n < m)$  is false.

Then, from the truth of (39-2), we can deduce that  $(\forall m \in \mathbb{N})(m \notin S_o)$  is true.

To show that, for all  $m$  in  $\mathbb{N}$ ,  $(\exists n \in \mathbb{N})(n \in S_o \wedge n < m)$  is false, let us show that, for all  $m$  in  $\mathbb{N}$ ,

$$\text{the denial of } (\exists n \in \mathbb{N})(n \in S_o \wedge n < m) \text{ is true.}$$

We use Mathematical Induction to show that a mathematical statement is true for all  $m$  in  $\mathbb{N}$ .

Thus, we need to define a subset  $E$  of  $\mathbb{N}$  that consists of all those natural numbers  $m$  such that the denial of  $(\exists n \in \mathbb{N})(n \in S_o \wedge n < m)$  is true. We use set-selector notation to display this set:

Let  $E := \{m \in \mathbb{N} : \sim (\exists n \in \mathbb{N})(n \in S_o \wedge n < m)\} = \{m \in \mathbb{N} : (\forall n \in \mathbb{N})(n \notin S_o \wedge n \geq m)\}$ . (Why the =?)

The defining criterion for membership in  $E$  consists of statements (one for each  $n$ ) of the form not- $A$  or  $B$ , where  $A$  denotes  $n \in S_o$  and  $B$  denotes  $n \geq m$ . Each of these is equivalent to a statement of the form  $A \Rightarrow B$ , so we can re-write the expression for  $E$  once again, as

$$E = \{m \in \mathbb{N} : (\forall n \in \mathbb{N})(n \in S_o \Rightarrow n \geq m)\}.$$

Let us express each one in the equivalent form not- $B \Rightarrow$  not- $A$ , so that we can write  $E$  in yet another way:

$$(39-4) \quad E = \{m \in \mathbb{N} : (\forall n \in \mathbb{N})(n < m \Rightarrow n \notin S_o)\}.$$

In words,  $E$  consists of all natural numbers  $m$  such that no natural number that is less than  $m$  belongs to  $S_o$ .

We know that  $0$  belongs to  $E$ , because for all  $n$  in  $\mathbb{N}$ , the antecedent (i.e.  $n < m$ ) in “ $n < m \Rightarrow n \notin S_o$ ” is false when  $m = 0$ .

To apply Mathematical Induction, we need to show that, for an arbitrary natural number  $m$ , “ $m \in E \Rightarrow m+1 \in E$ ” is true. We may suppose  $m \in E$ . This means that  $(\forall n \in \mathbb{N})(n < m \Rightarrow n \notin S_o)$  is true.

In order to show that, **necessarily**,  $m+1 \in E$ , we need to show that  $(\forall n \in \mathbb{N})(n < m+1 \Rightarrow n \notin S_o)$  is true.

This has the universal quantifier “ $\forall n \in \mathbb{N}$ .”

Therefore we need to show that, for an arbitrary  $n$  in  $\mathbb{N}$ ,  $n < m+1 \Rightarrow n \notin S_o$ .

By the Trichotomy Law, we can divide the work into three cases, depending on “where”  $n$  is, relative to  $m$ . In Case 1, we will assume  $n < m$ . In Case 2, we will assume  $n = m$ . In Case 3, we will assume  $n > m$ .

**Case 1:** In this case,  $n < m$ . This case does not occur if  $m = 0$  (why?). If  $m > 0$ , and  $n < m$ , then “ $n < m \Rightarrow n \notin S_o$ ” is true simply because  $m \in E$ . But then, since  $n < m$ , transitivity of inequality (**Exercise (23)**) shows that  $n < m + 1$ . Thus, for  $n < m$ ,  $n < m + 1 \Rightarrow n \notin S_o$  is true.

**Case 2:** In this case,  $n = m$ . We already know that no natural number smaller than  $m$  is in  $S_o$ . There are two possibilities, exactly one of which must be true, by the Law of the Excluded Middle:  $m \notin S_o$  and  $m \in S_o$ . The first of these is what we are trying to prove, so we have nothing to do if  $m \notin S_o$ . Thus we have to show that  $m \in S_o$  is false. Again we turn to a contradiction argument to prove it. Suppose, then, that  $m \in S_o$ . Then no natural number smaller than  $m$  is in  $S_o$ . Therefore, for every  $n$  in  $S_o$ ,  $m \leq n$ . We now recognize that this means  $m$  is the least element of  $S_o$ ! Since we assumed at the outset that that  $S_o$  does not have a least element,  $m$  cannot belong to  $S_o$ . Therefore, for  $n = m$ , “ $n < m \Rightarrow n \notin S_o$ ” is true.

**Case 3:** In this case,  $n > m$ . Therefore, there exists  $k$  in  $\mathbb{N}$ ,  $k \neq 0$ , such that  $n = m + k$ . By **Exercise (25)**,  $k \geq 1$ . Therefore, by transitivity,  $n \geq m + 1$ . Thus “ $n < m \Rightarrow n \notin S_o$ ” is vacuously true in this case.

We have shown that, if  $m \in E$  then  $(\forall n \in \mathbb{N})(n < m \Rightarrow n \notin S_o)$  is true. This completes the work needed to apply Mathematical Induction. Therefore,  $E = \mathbb{N}$ .

Let us now show that, because  $E = \mathbb{N}$ ,  $S_o$  is empty, so that we can get our contradiction. We will use the version (39-4) expressing  $E$ . Let’s suppose that  $S_o$  is not empty. Then there exists  $m_o$  in  $\mathbb{N}$  such that  $m_o \in S_o$ . Then  $m_o + 1 \in E$  because  $E = \mathbb{N}$ . Since  $m_o < m_o + 1$ ,  $m_o \notin S_o$ . This is a contradiction. Thus  $S_o$  is empty if (39-2) is true. Since we deduced (because of the contradiction assumption) that (39-2) is true, we now know that  $S_o$  is empty. But at the beginning of the argument, we assumed that  $S_o$  is NOT empty. This is a contradiction. Thus our assumption that there exists a non-empty set  $S_o \subseteq \mathbb{N}$  without a least element is false. Therefore, every non-empty subset  $S$  of  $\mathbb{N}$  has a least element. This completes the proof!

Here is a **shorter version** of the proof, without all the explanations, that is suggested by the proof just given: Let  $S_o$  be a non-empty subset of  $\mathbb{N}$ . Suppose that  $S_o$  does not have a least element. Let  $E$  be given by (39-4). If we can show that  $E = \mathbb{N}$ , we can contradict the assumption that  $S_o$  is non-empty. Let  $m = 0$ . The statement  $n < m \Rightarrow n \notin S_o$  is vacuously true if  $m = 0$ . Thus,  $0 \in E$ . Now suppose  $m \in E$ . To show that  $m + 1 \in E$ , it is enough to show that  $m \notin S_o$ . Suppose not. That is, suppose  $m \in S_o$ . Then, since no element of  $\mathbb{N}$  that is smaller than  $m$  is in  $S_o$ ,  $m$  is the least element of  $S_o$ . This contradicts our initial assumption. Thus,  $m \notin S_o$ . Hence, no natural number smaller than  $m + 1$  is in  $S_o$ . This shows that  $m + 1$  is in  $E$ , and so by Mathematical Induction,  $E = \mathbb{N}$ . But this implies that  $S_o$  is empty, because, if some  $m_o \in S_o$ , the fact that  $m_o + 1 \in \mathbb{N}$  implies that  $m_o + 1 \in E$ , since  $E = \mathbb{N}$ . But  $m_o + 1 \in E$  implies that  $m_o \notin S_o$ . This is a contradiction. Thus  $S_o$  is empty. This is a contradiction. Thus every non-empty subset of  $\mathbb{N}$  has a least element.

### An application of the Well-Ordering Theorem

There is another version of the Principle of Mathematical Induction that is sometimes useful. It uses inequalities in its statement.

(40) **Theorem (The “ordinal” form of the Principle of Mathematical Induction):** Suppose that for each  $n \in \mathbb{N}$   $P(n)$  is a mathematical statement with variable  $n$ . Suppose also that we are given:

(1)  $P(0)$  is true

and that

(2) for all  $n \in \mathbb{N}$ , if  $P(m)$  is true for all  $m \in \mathbb{N}$  such that  $m < n$ , then  $P(n)$  is true.

Then  $P(n)$  is true for all  $n \in \mathbb{N}$ .

(41) **Exercise:** In the Theorem, is (1) redundant? Why?

*Proof of the Theorem:* Suppose that (1) and (2) hold (i.e., are true) but that  $P(n)$  is not true for every  $n \in \mathbb{N}$ . We define  $E = \{n \in \mathbb{N} : P(n) \text{ is false}\}$ . By our contradiction assumption,  $E$  is not empty. By the Well-Ordering Principle,  $E$  has a least element, which we can call  $m_o$ . By (1),  $m_o \neq 0$ . Thus  $m_o > 0$ , and by the definition of  $E$ ,  $P(m)$  is true for every  $m < m_o$ . But then by (2),  $P(m_o)$  is true and so  $m_o \notin E$ . This is a contradiction! Thus  $E$  is empty, and  $P(n)$  is true for all  $n \in \mathbb{N}$ .

This is as far as we will go along this path. What follows is included so you can see how the development continues.

(42) **Special Problem:** Prove the following Theorem–with–Definition and notation.

**Theorem and Definition (of) and notation (for) ([on] multiplication):** *There exists one and only one function  $t : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  with the following properties:*

(A) for all  $n$  in  $\mathbb{N}$ ,  $t(n, 1) = n$ ;

(B) for all  $n$  in  $\mathbb{N}$ , and for all  $m$  in  $\mathbb{N}$ ,  $t(n, s(m)) = p(n, t(n, m)) = n + t(n, m)$ .

We call the finding of the value of  $t(n, m)$  *multiplication of  $n$  and  $m$* , and we call the value of  $t(n, m)$  *the product of  $n$  and  $m$* . We use the notations  $nm := t(n, m)$ ,  $n \cdot m := t(n, m)$ ,  $n \times m := t(n, m)$ . We won't use the second and third notations much.

To do this problem, you might use the proof of the theorem about addition as an outline, and make appropriate changes.

(43) **Exercise:** Show that for all  $n$  in  $\mathbb{N}$ ,  $n \cdot 0 := t(n, 0) = 0$ .

(44) **Exercise:** Show that multiplication is associative.

(45) **Exercise:** Show that multiplication is commutative.

(46) **Problem:** Show that multiplication distributes over addition, that is,  $n(k + \ell) = nk + n\ell$ , a statement also known as the Distributive Law. Include the right quantifiers!

(47) **Exercise:** Show that, if  $m$  and  $n$  are in  $\mathbb{N}$ , and  $nm = 0$ , then  $n = 0$  or  $m = 0$ . You might want to prove, instead, that “ $n \neq 0$  and  $m \neq 0$ ” implies “ $nm \neq 0$ ” is true. Do you agree that the two statements are equivalent? This is also known as the Cancellation Law (for multiplication by a non-zero natural number). This is called the Cancellation Law because it is logically equivalent to the next **Exercise**.

(48) **Exercise:** Show that, if  $m$ ,  $n$  and  $p$  are in  $\mathbb{N}$ , and  $n \neq 0$ , then “ $nm = np$  implies  $m = p$ ” is true. This is the theorem that is usually called the Cancellation Law (for multiplication by a non-zero natural number).

(49) **Exercise:** There is a Cancellation Law for addition too. State it, and prove it. (Hint: This has been done in a previous exercise; if you haven't done it yet, now's the time!)

(50) **Theorem and Definition (The Division Algorithm):** *Let  $n$  be a non-zero natural number, and let  $m$  be a natural number. Then there exist unique natural numbers  $q$  and  $r$  such that  $0 \leq r < n$ , and  $m = qn + r$ . The number  $q$  is called the quotient, and the number  $r$  the remainder, (when  $m$  is divided by  $n$ ).*

(51) **Definition and notation:** Let  $m \in \mathbb{N}$ ,  $n \in \mathbb{P}$ . Then  $m$  is divisible by  $n$  if there exists  $q$  in  $\mathbb{N}$  such that  $m = nq$ . We express this in symbols by  $n|m$ . We also say that  $n$  is a divisor of  $m$ .

(52) **Exercise:** Show that “is divisible by” is a transitive and reflexive relation on  $\mathbb{P}$ .

(53) **Exercise:** Show that “is divisible by” is not a symmetric relation on  $\mathbb{P}$ .

(54) **Exercise:** Suppose  $n \in \mathbb{P}$ . Show that 0 is divisible by  $n$ .

(55) **Exercise:** Suppose  $m \in \mathbb{P}$  and  $n \in \mathbb{P}$ . Show that, if  $m$  is divisible by  $n$ , then  $n \leq m$ .

(56) **Exercise:** Suppose  $n \in \mathbb{P}$ . Do the last two **Exercise**s together imply  $n \leq 0$ ? Why not?

(57) **Definitions:** Let  $m \in \mathbb{N}$ . Then  $m$  is *even* if  $m$  is divisible by 2, and *odd* otherwise.

## References

- [1] Blackburn, Leonard, *Notes and Comments on the Addition Theorem* (soon to be posted on the course Web site).
- [2] Halmos, P. R., *Naive Set Theory*, Springer-Verlag, 1974. ISBN 0-387-90092-6.
- [3] Landau, Edmund, *Foundations of Analysis*, Chelsea, 1951.